UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,344	08/16/2001	Massimiliano Antonio Poletto	12221-004001	2635

26161 7590 02/06/2008
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
02/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,344
Filing Date: August 16, 2001
Appellant(s): POLETTO ET AL.

Denis Maloney
Reg. No.29, 670
Of
Fish & Richardson P.C.

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/24/2007 appealing from the Office action mailed 6/26/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,990,591	Pearson	12-1999
7,120,931	Cheriton	10-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

1. *Claims 1, 16, and 29 are provisionally rejected on the ground of nonstatutory double patenting over claims 1, 9, 18, and 21 are of copending Application No. 09/931,291. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.*

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on

that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows:

Claims 1, 16, and 29 of '344 recites a gateway disposed between a data center and a network for thwarting denial of service attacks on the data center Claims 1, 9, 18, and 21 of '291 reciting a computer system to coordinate thwarting attacks on a data center that is coupled to a network and further discloses the process to identify gateways on the monitoring network that are resources of malicious traffic destined for the data center. Thus, '344 and '291 obviously uses gateways for monitoring attacks towards the data center.

Both '344 and '291 recites communication of statistics collected from the monitoring process that obviously involves network traffic, attacks, etc. Further, '344 disclose the gateway comprises a computing device disposed between a data center and a network where the gateway is obviously separate or physically apart from the data center and the network because the gateway is disposed between the data center and the network. This obviously reads on '291 where plurality of monitors is physically separate network from the network that the data center is couple to.

Claims 1, 16, and 29 of '344 recite a filtering process to insert filters on network devices to filter out packets that deems to be part of an attack. Claims 1, 9, 18, and 21 of '291 recites network flows collected by plurality of monitors and analyzing the statistical data from the plurality of monitors to determine network

traffic statistics that can identify malicious network traffic. The plurality of monitors of '291 is obviously a broader variation to the filters of '344 because both applications claim a filtering process but '291 analyzes the traffic and '344 filters out the traffic that is considered an attack or malicious. Therefore, it would have been obvious the limitations of '344 read on '291 because both applications monitor network traffic to thwart attacks on a data center.

2. *Claims 1, 16, and 29 are provisionally rejected on the ground of nonstatutory double patenting over claims 1, 3, and 4 are of copending Application No. 10/066,252. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.*

As for '344, claim 1 recites a gateway disposed between a data center and a network for thwarting denial of service attacks on the data center. Claim 16 and 29 recites a victim site that is being protected from denial of service attacks and claim 16 additionally recites disposing a gateway between the victim site and a network. Thus, the victim site can broadly be given as a data center because both are being protected from denial of service attacks.

As for '*252*, claim 1 recites a device coupled to physical links between the data center and a network with the device disposed to examine traffic entering or leaving that data center on the couple physical links and collect statistical information.

The device of '*252* can broadly interpret as a gateway device of '344 because both devices are coupled between a data center and a network for monitoring and collecting traffic. Further, the difference between claims 1, 3, and 4 of '*252* to claims 1, 16, and 19 of '344 is that '344 do not include physical links. Physical links obviously is for one device to couple to other devices such as a gateway device coupled to physical links to the data center of claim 1 of '344 in order for communication of traffic to monitor the traffic of the network. Therefore, it would

have been obvious the combined limitations from claims 1, 3 and 4 of '*252* reads on claims 1, 16, and 19 of '344 because there includes monitoring, examining, and collecting network traffic for thwarting denial of service attacks on the data center.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. *Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson (US 6,990,591), in view of Cheriton (US 7,120,931).*

As per claim 1:

Pearson discloses a gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:

a monitoring process that monitors network traffic through the gateway;

(col.6, lines 6-19; *Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refer to the communication device 106.*)

a communication process that communicate statistics collected in the gateway from the monitoring process (col.8, lines 10-15 and col.19, lines 45-50) with a control center and that receives queries or instructions from the control center; (col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; *Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).*)

and *[a filtering process to insert filters on network devices to filter out packets]* that the gateway deems to be part of an attack. (col.9, lines 11-16 and col.16, lines 36-53)

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col.10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels. Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks (col.9, lines 11-16 and

col.16, lines 36-53). However, Pearson did not particularly discuss a filtering process to insert filters on network devices to filter out the threats.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43)

and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53).

As per claim 2: See Pearson on col.3, lines 59-65 and col.12, lines 30-33; discussing the communication process couples to a dedicated link to communicate with the control center over a hardened network.

As per claim 3: See Pearson on col.1, lines 52-60; discussing the monitoring process in the gateway samples network packet flow in the network.

As per claim 4: See Pearson on col.15, lines 18-20 and col.16, lines 34-36; discussing the gateway is adaptable to be physically deployed in line in the network.

As per claim 5: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing the gateway is adaptable to dynamically install filters on nearby routers.

As per claim 6: See Pearson on col.18, lines 51-67; discussing the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 7: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 8: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram

Protocol (UDP) packets to unused ports.

As per claim 9: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 10: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

As per claim 11: See Pearson on col.11, lines 8-12 and Cheriton on col.7, lines 32-65; discussing monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

As per claim 12: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 13: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

As per claim 14: See Pearson on col.11, lines 31-35; discussing monitoring process logs packets.

As per claim 15: See Pearson on col.11, lines 40-57 and col.18, lines 22-24;

discussing monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

As per claim 16:

Pearson discloses a method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network; (col.6, lines 6-19; *Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refer to the communication device 106.*)

monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic; (col.8, lines 10-15 and col.19, lines 45-50)

communicating the statistics collected in the gateway to a control center; (col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; *Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).*)

[and filtering out packets] that the gateway or control center deems to be part of an attack. (col.9, lines 11-16 and col.16, lines 36-53; *Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks.*)

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col.10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels. However, Pearson did not particularly discuss a filtering out packets that the gateway or control center deems to be part of an attack.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a

group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53).

As per claim 17: See Pearson on col.3, lines 59-65 and col.12, lines 30-33; discussing communicating occurs over a dedicated link to the control center via a hardened network.

As per claim 18: See Pearson on col.1, lines 52-60; discussing monitoring samples network packet flow in the network.

As per claim 19: See Pearson on col.15, lines 18-20 and col.16, lines 34-36; discussing the gateway is physically deployed in line in the network.

As per claim 20: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing filtering further comprises: dynamically installing filters on nearby routers via an out of band connection.

As per claim 21: See Pearson on col.18, lines 51-67; discussing monitoring further

comprises: detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 22: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 23: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing monitoring further comprises: detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 24: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing monitoring further comprises: detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 25: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing monitoring further comprises: detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

As per claim 26: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing monitoring further comprises: logging statistics on parameters including source and destination host or network addresses, protocols, types of packets,

number of open connections or of packets sent in either direction.

As per claim 27: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing monitoring further comprises: issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 28: See Pearson on col.11, lines 40-57 and col.18, lines 22-24; discussing monitoring further comprises: logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

As per claim 29:

Pearson discloses a computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic; (col.6, lines 6-19; *Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refer to the communication device 106.*)

communicate statistics collected (col.8, lines 10-15 and col.19, lines 45-50) in the computer device to a control center; and (col.7, lines 55-62; col.9, lines 11-17; *FIG.1 (controller 112); and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130*

comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col.15, lines 52-65 and col.16, lines 26-29).)

[filter out packets] that the device or control center deems to be part of an attack. (col.9, lines 11-16 and col.16, lines 36-53; *Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks.)*

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col.10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co.11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col.18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels. However, Pearson did not particularly discuss a filtering out packets that the gateway or control center deems to be part of an attack.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the

network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53).

As per claim 30: See Pearson on col.1, lines 52-60; discussing sample network traffic flow.

As per claim 31: See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing instructions to filter further comprise instructions to: dynamically install filters on nearby routers via an out of band connection.

As per claim 32: See Pearson on col.18, lines 51-67; discussing instructions to monitor further comprise instructions to: detect IP traffic; and determine levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

As per claim 33: See Pearson on col.17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

As per claim 34: See Pearson on col.17, lines 47-47 and Cheriton on col.6, lines 10-18; discussing instructions to monitor further comprise instructions to: detect Internet Protocol (IP) traffic; and determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

As per claim 35: See Pearson on col.8, lines 16-25 and Cheriton on col.8, lines 1-44; discussing instructions to monitor further comprises instructions to: detect IP traffic; and determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

As per claim 36: See Pearson on col.10, lines 33-38 and Cheriton on col.8, lines 30-44; discussing instructions to monitor further comprises instructions to: detect a sustained rate of reload requests that is higher than plausible for a human user

over a persistent HTTP connection.

As per claim 37: See Cheriton on col.5, lines 20-25 and col.7, lines 32-col.8, line 10; discussing instructions to monitor further comprises instructions to: log statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

As per claim 38: See Pearson on col.8, lines 10-32 and col.17, lines 1-10; discussing instructions to monitor further comprises instructions to: issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

As per claim 39: See Pearson on col.11, lines 40-57 and col.18, lines 22-24; col.7, lines 43-55; discussing instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway.

(10) Response to Argument

Claims 1-39 are rejected under 35 U.S.C. 103(a) as being obvious over the Pearson and Cheriton combination. Throughout the Appeal Brief, appellant did not point to particular citations to specify what exactly that Pearson and Cheriton fails to teach or teach against that correspond to the claimed limitations being traversed. Appellant pointed to a couple of citations on pg.16-17, but throughout pgs.7-20 merely copy/paste examiner's rejection and passages from the prior arts without

noting its column and lines relating to the traversal. Thus, examiner herein will respond in accordance with the claimed invention and to the best understanding in response to appellant's arguments and points discussed in this appeal brief.

According to claim 1: *Examiner traverses the argument throughout pages 7-10, where Pearson in combination with Cheriton neither describes nor suggests claim 1 particularly a computing device that includes a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center.*

Pearson discloses a communication device 106 such as a gateway, firewall, or other devices that communicates data between one or more ports (col.6, lines 5-9). Hence, the claimed gateway can be given in light as Pearson's communication device 106. Pearson discloses a remote monitoring center (RMC) as the claimed control center where the communication device (gateway) transmit the type of communication causing the alert to the RMC for analysis and handling (col.3, lines 5-8).

Statistics can reasonably be interpreted as the relationship among groups of measurement and with relevance of similarities and differences in those relationships. As such, it is known in the art that DoS attacks are determined on their similarities and differences measured amongst the network traffic. As for Pearson, the communication device implements intrusion detection functionality via

intrusion detector 160 and determining whether such communications comprise an attack or other security risk (i.e. DoS) by comparing to a list (col.8, lines 10-25 and col.17, lines 8-22). Pearson suggests the data collected in the communication device comprises attacks or other security risk (i.e. DoS) from monitoring the network in the gateway as collected statistics.

Pearson discloses the communication device transmit a type of communication causing the alert (col.3, lines 5-8) and the RMC receive the signal or message indicative of an attack which then create a communication to the RMC (col.7, lines 59-62). With Pearson able to determine whether such communications comprise an attack or other security risk (i.e. DoS) (col.8, lines 10-25 and col.17, lines 8-22), obviously suggests sending statistics in the signal collected in the gateway to the control. Thus, the gateway communicating a signal to the control center (RMC) is not merely for signaling an alert, but is a message with statistics indicative of an attack. Further, Pearson discloses transmitting a wake-up signal to the RMC comprising diagnostic variables associated with the operations of the communication device and other parameter indicative of the state of operations of the communication devices where the RMC receives the signal and records the information contained in the signal and compares the information with a list (col.3, lines 63-67 and col.12, lines 40-45). Hence, once again Pearson suggests the signal includes data in order for the RMC to compare against with a list rather than just a carrier wave form utilized solely for warning or alerting. In addition, Pearson

indicates that all communications from the communication device may be transmitted and recorded at RMC for subsequent analysis (col.18, lines 1-10). Pearson discloses the violated rule is transmitted to the RMC that constitutes message body and any other information associated with the violation that the RMC wish to log and inspect (col.20, lines 40-50). Accordingly, this communication suggests violation information being sent to the RMC for inspection and not just a mere signaling to alert the RMC.

Thus, in light of the broad and reasonable interpretations in accordance with claim 1 as discussed above, examiner concludes that Pearson suggests whether a signal, or message (col.3, lines 5-8 and col.7, lines 59-62), or violated rule (col.20, lines 40-50) is a type of communication that includes statistics (of DoS attacks) collected in the gateway whereby (col.8, lines 10-25 and col.17, lines 8-22) causing an alert to the RMC for further comparison and inspections (col.12, lines 40-45 and col.18, lines 1-10). Therefore, Pearson reads on the claimed communication process that communicates statistics collected in the gateway from the monitoring process with a control center and receives queries or instructions from the control center.

Regarding the argument on pg.10 (2nd paragraph), *examiner traverses that Pearson neither describers nor suggests the control center queries the gateway for the statistical information.* Claim 1 recites a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center.

This limitation can broadly and reasonably suggest the control center (RMC) sending queries or instructions to the gateway. However, the claimed invention does not particularly limit what the control center is querying or instructing for, i.e. statistical information as appellant argued. Hence, claim 1 does not read nor broadly suggest the control center queries for statistical information.

Further, regarding the argument on pg.10 (3rd paragraph), *traverses Pearson is directed to the alert signal is misplaced and raising alerts.* As discussed earlier, the RMC receiving the alert signal is not merely signaling alerts but the signal, or message (col.3, lines 5-8 and col.7, lines 59-62), or violated rule (col.20, lines 40-50) is a type of communication that includes statistics data (of DoS attacks) collected in the gateway whereby (col.8, lines 10-25 and col.17, lines 8-22) causing an alert to the RMC for further comparison and inspections (col.12, lines 40-45 and col.18, lines 1-10).

Regarding arguments on pgs.10-11, *that Cheriton does not cure any deficiencies in the teachings of Pearson because Cheriton does not query a gateway from a control center for statistical information on network flows.* Pearson is the primary art that teaches monitoring network traffic through the gateway and collecting statistics (i.e. Denial of Service Attacks or DoS) in the gateway whereby communicating the signal, message (col.3, lines 5-8 and col.7, lines 59-62), or violated rule (col.20, lines 40-50) includes data (statistics of DoS attacks) collected in the gateway (col.8, lines 10-25 and col.17, lines 8-22) causing an alert to the RMC

for further comparison and inspections (col.12, lines 40-45 and col.18, lines 1-10). Pearson vaguely discusses filtering out threats (col.11, lines 1-20 and col.19, lines 45-53). Hence, Pearson suggests all elements of claim 1 except a filtering process to insert filters on network devices. Thus, Cheriton is brought forth to combine with Pearson to teach the filtering process to insert filters on network devices to filter out the threats.

In short summary, Cheriton discloses a method and system for analyzing network flows using a filter at a network device (col.2, lines 29-43) for identifying and analyzing packets based on statistics (col.7, lines 32-60 and col.8, lines 12-65) to prevent harmful network flows (i.e. DoS attacks) from passing through into the network (col.3, lines 38-53). Therefore, it would have been obvious for a person of ordinary skills in the art to modify Pearson with Cheriton to teach inserting the filter in a firewall/gateway to analyze harmful network flows to prevent network flows from passing through the network device (Cheriton-col.2, lines 29-43) and data incoming is filtered to reduce the possibility of problems in the network (Cheriton-col.3, lines 38-53).

Claims 2-15 are also rejected by virtue of their dependency to claim 1 in view of Pearson and Cheriton combination.

According to claim 29:

Regarding the argument on pg. 12 (paragraph), *Pearson fails to suggest instructions to communicate statistics collected in the computer device to a control*

center, rather Pearson discloses attack signatures. Pearson discloses examples of intrusions, attacks, or violations may be in forms of attack signatures or Denial of Service attacks (DoS) (Pearson-col.8, lines 10-45 and col.19, lines 45-55). Statistics can reasonably interpret as the relationship among groups of measurement and with relevance of similarities and differences in those relationships. Both Pearson (Pearson-col.2, lines 45-67 and col.6, lines 5-30 and col.8, lines 10-67) and Cheriton (Cheriton-col.1, lines 40-57 and col.8, lines 12-65) discloses monitoring network traffic and analyzing incoming communications for potential security breaches or intrusions (i.e. DoS attacks). Thus, the DoS are determined on similarities and differences measured amongst the network traffic. Therefore, Pearson and Cheriton combination reads on the claimed measure heuristics of the network traffic in the computer device to provide statistics on the network traffic to a control center (RMC) as claimed.

Claims 30-39 are also rejected by virtue of their dependency to claim 29 in view of Pearson and Cheriton combination.

According to claim 16:

Regarding the argument on pg. 16-17 (paragraph), appellant did not address the rejection of independent claim 16 separately, but rather argued together with independent claim 1. Hence, refer to examiner's response above regarding claim 1. Claims 17-28 are also rejected by virtue of their dependency to claim 16 in view of Pearson and Cheriton combination.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Leynna Ha (Patent Examiner, GAU 2135)

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron (SPE 2132)

/Benjamin Lanier/
Benjamin Lanier (Primary Examiner, GAU 2132)